# 修 士 論 文 の 和 文 要 旨

| | | | |
|---|---|---|---|
| 研究科・専攻 | 大学院情報システム学研究科情報ネットワークシステム学専攻 博士前期課程 | | |
| 氏　　名 | 大島 崇司 | 学籍番号 | 0952003 |
| 論 文 題 目 | 分散ハッシュテーブルと Crowds による双方向匿名通信路の提案 | | |


要　旨

双方向匿名通信の新規手法を提案する．論文で目的とする双方向匿名性とは，通信を行う際に受信者と送信者が互いの IP アドレスを知り得ることが無く，またその他の通信に関わる者全てが受信者と送信者の IP アドレスを知り得ないこととしている．

この研究の背景には，インターネットプロトコルの IPv4 から IPv6 への移行，また Peer to Peer 通信の機会拡大などにより，IP アドレスを隠ぺいしたまま通信する必要性が高まっていることがある．選挙や医療情報，GPS 位置情報を含んだ通信など，高い匿名性が必要とされる通信での利用が考えられる．

匿名通信の従来手法では，多重暗号化を用いて送信者を匿名とする通信手法や，分散ハッシュテーブルを用いて大規模な匿名通信を実現するための方法が研究されている．これにより，送信者の匿名性を，受信者やその他全ての通信に関わる者に対して確保する通信が可能となっている．しかし，上に挙げた用途などを想定するとこれだけでは不十分であると考えられる．従来手法では受信者に同様の匿名性を付与することが難しいからである．送信者同様，受信者にも高い匿名性が必要である．尚，双方向匿名通信の既存研究として，匿名にファイル共有を行う手法が複数提案されている．しかし，これらの手法ではファイルが入手できれば相手は誰でもよく，特定の相手を指定しての一般的な通信を匿名に行うことはできない．

本論文では，匿名通信についてどのような研究がされてきたか示した．その上で，双方向匿名通信路構築の新規手法について提案した．提案手法とは，送信者の IP アドレスと受信者の IP アドレスを，通信に関わる自分以外の全ノード（送信者・受信者も含む）に対して秘匿する（名前と IP アドレスを紐づけることができない）ものであった．これにより送信者・受信者が互いに同程度の匿名性を持つ通信が可能なため，匿名通信でメッセージを送ってきた相手に対して，後でその者の名前を検索することで再び見つけて返信を行うことが可能になる．以上の提案により，一般的な通信を双方向に匿名化する手法を示した．